

# **Hard Drive of Hearing: Disks that Eavesdrop with a Synthesized Microphone**

**Andrew Kwong, Wenyuan Xu, Kevin Fu**

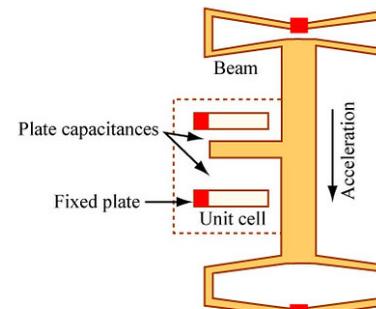
[andrewkwong.org](http://andrewkwong.org), [usslab.org](http://usslab.org), [spqr.eecs.umich.edu](http://spqr.eecs.umich.edu), [kevinfu@umich.edu](mailto:kevinfu@umich.edu)

IEEE Symposium on Security and Privacy 2019  
Grand Ballroom B -- 1:10Pm



# Sensors Intrude on Privacy

- Accelerometers can leak keystrokes [1], gyroscopes can leak voice [2], etc.
- What is the threat from devices never intended to be sensors in the first place?



Accelerometers: [1] Marquardt et al., CCS '11, "(sp)iPhone..."

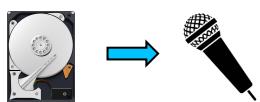
Gyroscopes: [2] Michalevsky et al., Usenix Security '14, "Gyrophone..."

# Hard Drive as a Microphone?



## Challenges:

- HDDs are not designed as microphones
- Large quantity of self-noise
- Low signal-to-noise ratio



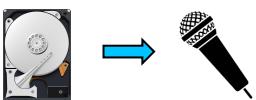
# Contributions

## HDD as a microphone

- Used SNReval measurements to evaluate extracted speech quality
- Used Shazam to recognize song recovered through HDD

## Mitigations

- Ultrasonic aliasing
- Firmware signatures



# Threat Model

## Firmware Resident Malware

- Drive firmware can be flashed from software

### Flashing:

- MITM attacks (POODLE, LOGJAM, DROWN)
- Any compromise granting root access to a machine

2007

EDITION: US ▾

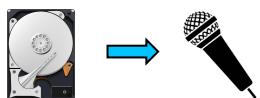
The screenshot shows a news article from ZDNet. At the top, there's a dark header bar with the ZDNet logo, a search icon, and navigation links for 'VIDEOS', '5G', and 'WINDOWS 10'. Below the header, a light gray banner displays the text 'MUST READ: Facebook's Mark Zuckerberg: "The future is private"' in red. The main title of the article is 'Malware found on new hard drives' in large, bold black font. Below the title, a paragraph of text discusses a story from the Taipei Times about Maxtor external hard drives being shipped with malware. At the bottom of the article, there's a small profile picture of the author, Adrian Kingsley-Hughes, and the text 'By Adrian Kingsley-Hughes for Hardware 2.0 | November 13, 2007 -- 14:10 GMT (06:10 PST) | Topic: Security'.

## Malware found on new hard drives

The Taipei Times is reporting that around 1,800 new 300GB and 500GB external hard drives manufactured by Maxtor shipped with malware on them. What makes this story even more interesting is that Taiwanese authorities suspected that Chinese authorities were involved.



By Adrian Kingsley-Hughes for Hardware 2.0 | November 13, 2007 -- 14:10 GMT (06:10 PST) | Topic: Security



EDITION: US ▾

ZDNet 

VIDEOS 5G WINDOWS 10 CLOUD AI INNOVATION SECURITY MORE ▾ NEWSLETTERS ALL WRITERS 

MUST READ: IT strategy: How an investment in diversity can boost your business

# Apple's T2 security chip disconnects a MacBook's microphone when users close the lid

Feature only available for MacBook Pro and MacBook Air models released in 2018.



By Catalin Cimpanu for Zero Day | October 30, 2018 -- 20:00 GMT (13:00 PDT) | Topic: Security



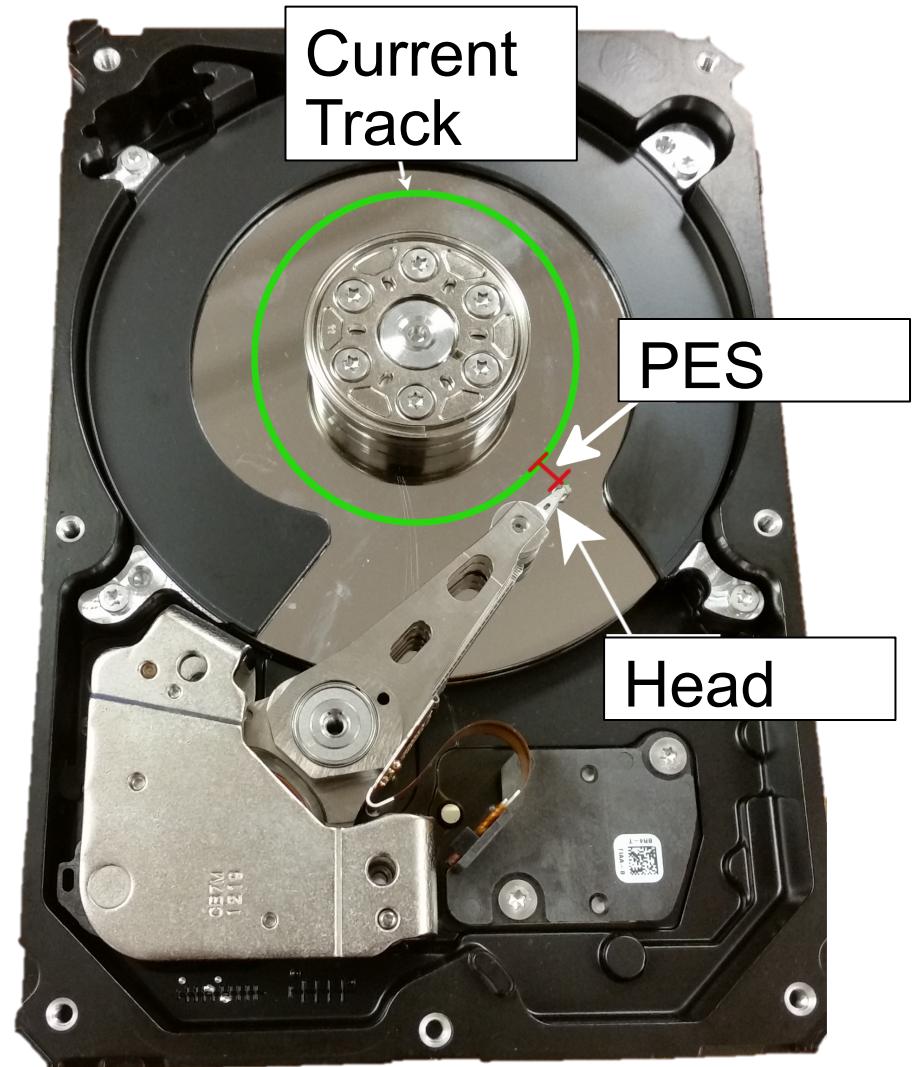
<http://stahlke.org/dan/phonemute/>



Andrew Kwong (<https://andrewkwong.org>)

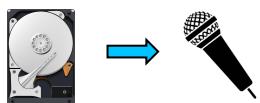
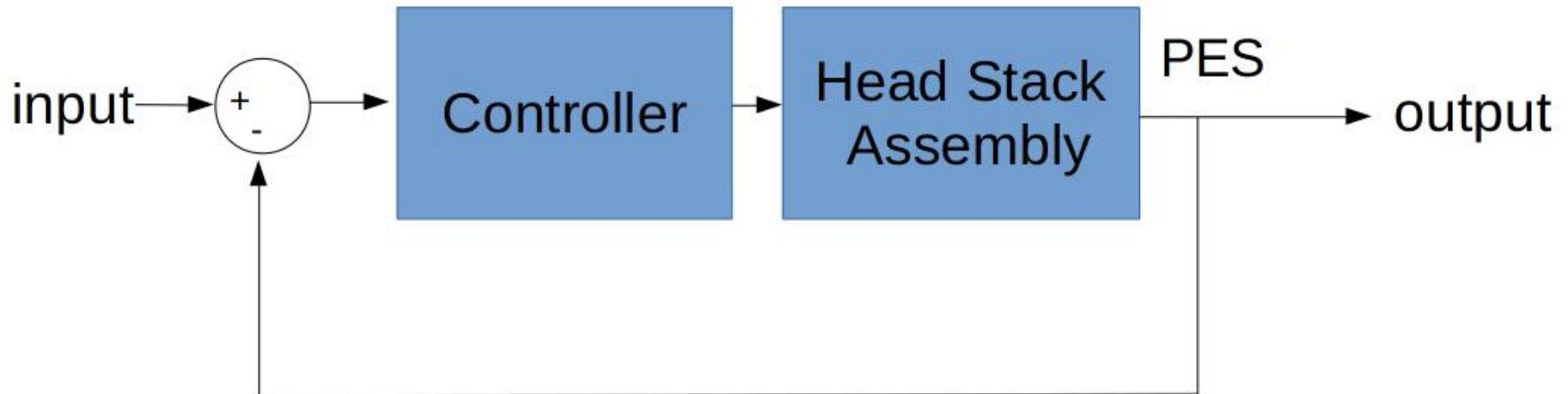
# HDD as a microphone

- Head stack assembly actuates the read/write head as the disk spins beneath it
  - Head follows a track
  - can tolerate only tiny errors
- Position Error Signal(PES):
  - Head's offset from center of current track

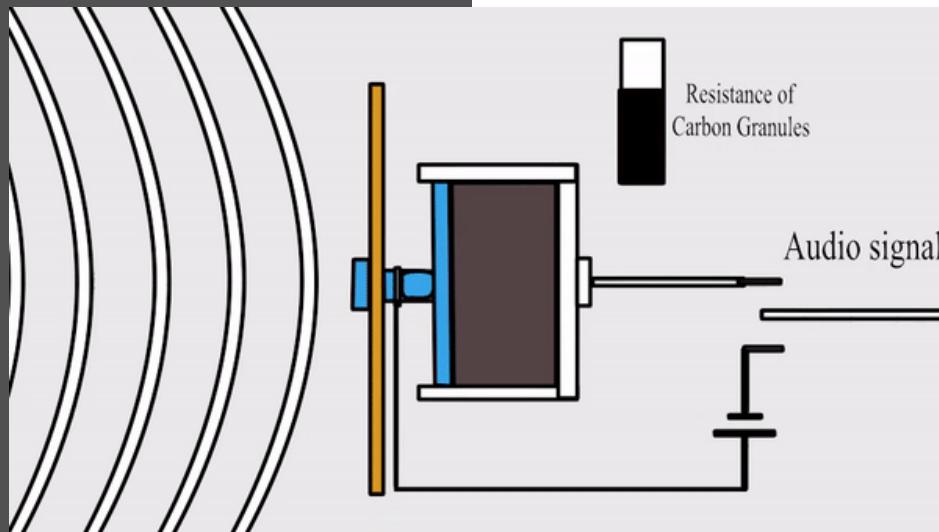


# Head Tracking

- Utilizes Feedback-Control Loop to keep head on track
- Generates PES by reading out magnetic burst from servo sectors
  - Fixed number of servo sectors per track



# Similarities to Microphone



<https://www.instructables.com/id/Simplified-Electronics-Microphone-DIY-How-It-Works/>

## Microphone:

- Output measures diaphragm displacement
- Sound waves displace diaphragm

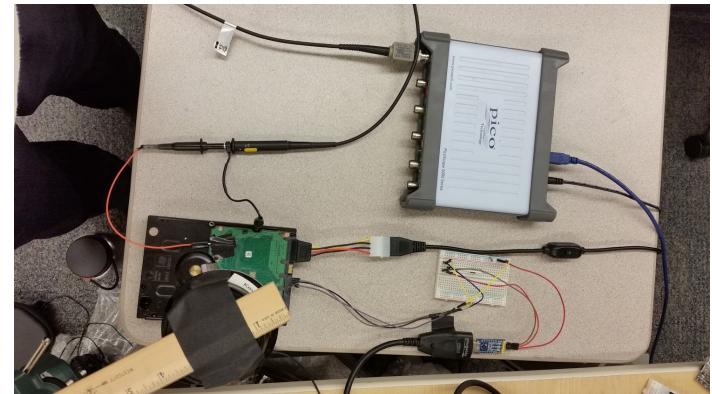
## HDD:

- PES measures read/write head displacement
- Sound waves displace write head?

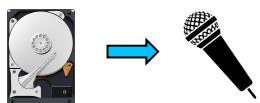
**PES approximates  
microphone output??**

# Measuring the PES

- Under our threat model, attacker would read it through firmware resident malware
  - Zaddach et al. [3] developed HDD firmware malware
- Proof of concept: suffices to read PES by tapping a debug pin
  - Used serial diagnostic port to output PES



HDD Malware: [3] Zaddach et al., ACSAC '13



# Sampling Rate

$$\begin{aligned}\text{frequency}_{\text{sampling}} &= \text{frequency}_{\text{rotation}} * \text{num\_servo\_sectors\_per\_track} \\ &= 120 \text{ Hz} * 288 \\ &= 34,560 \text{ Hz}\end{aligned}$$

Nyquist-Shannon Sampling theorem:

- need sample at 2x the frequency of signal

Audible sound: 20 Hz-20 kHz

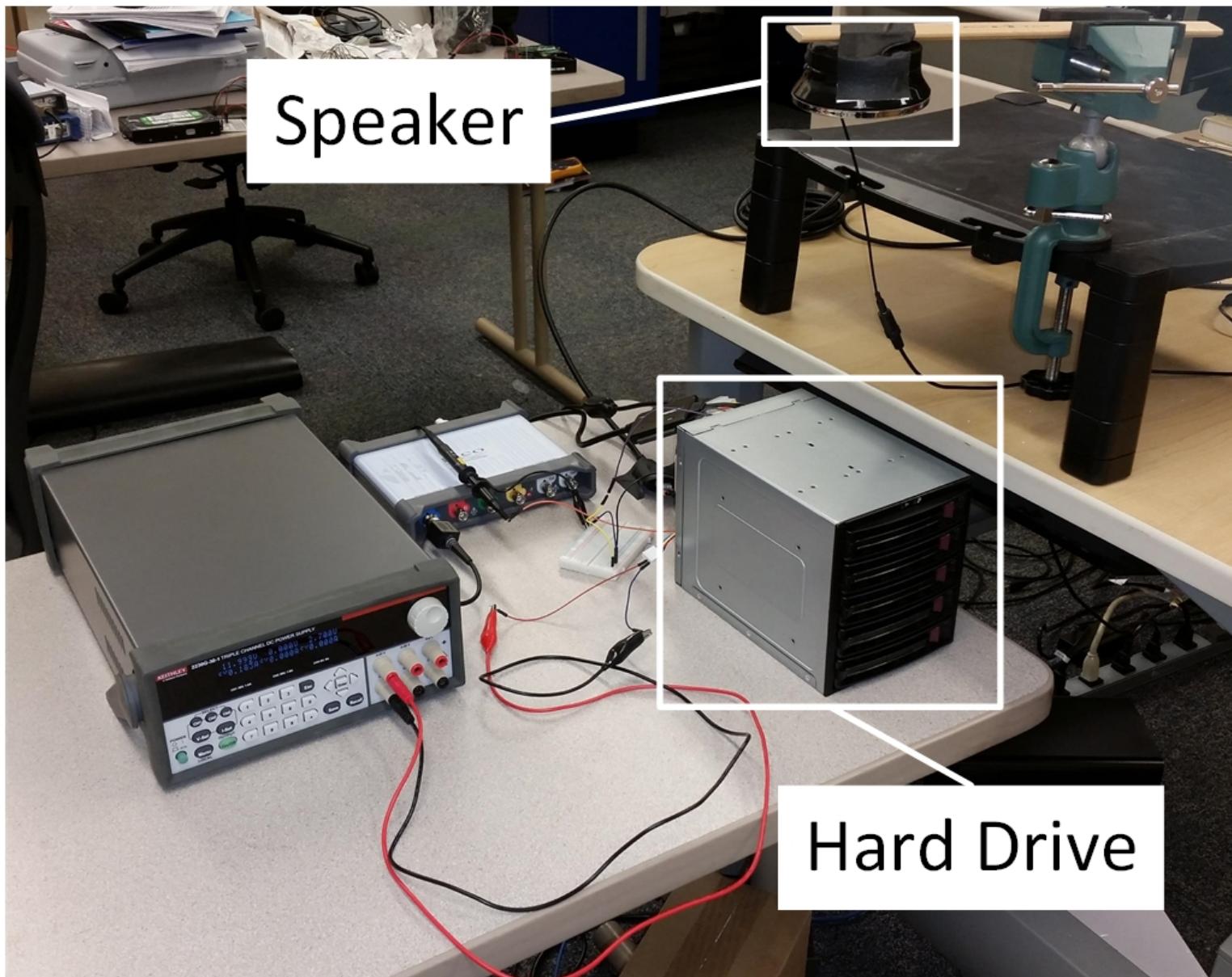
- Male fundamental: 85-180 Hz
- Female fundamental: 156-255 Hz
- POTS: 8 kHz



# demo



# Experimental Setup



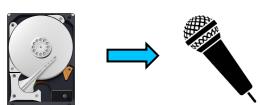
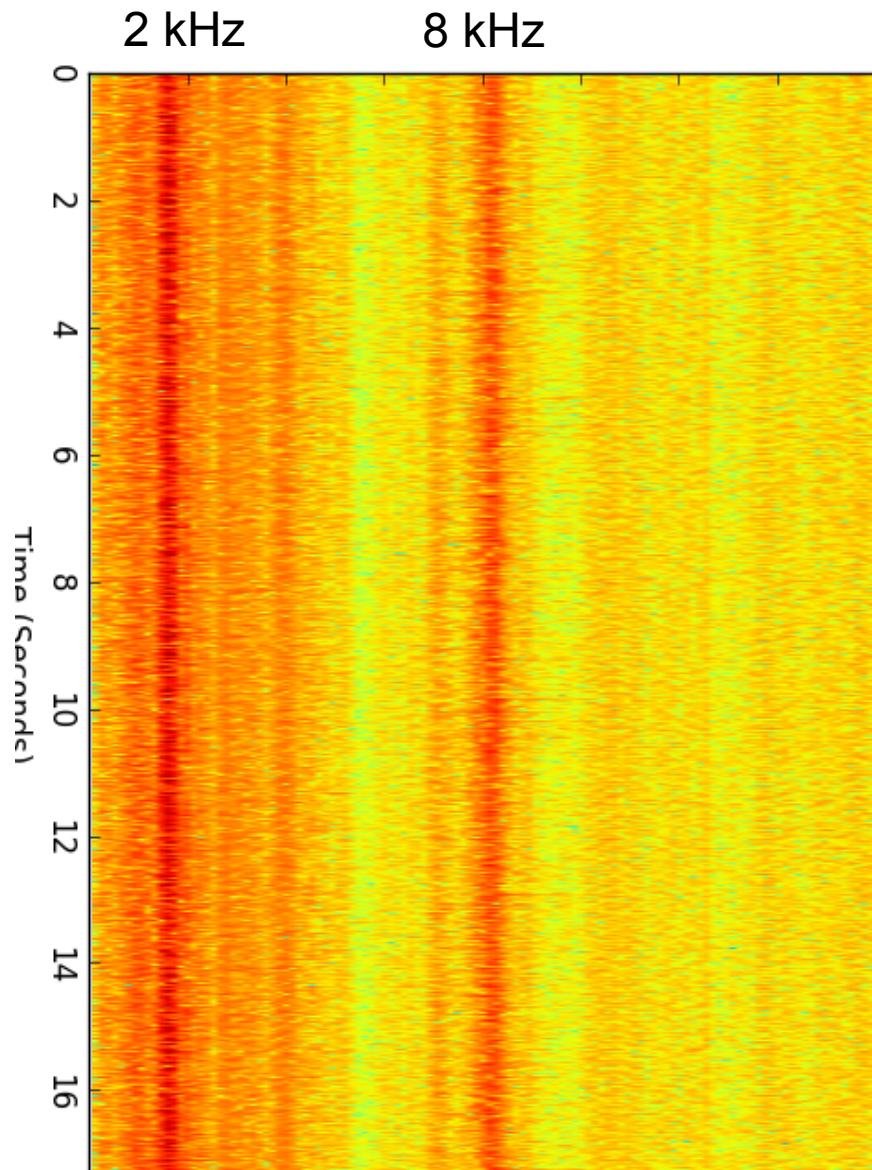
# Speech Recovery

Must recover speech from PES readings

- PES values approximate instantaneous air pressure readings
- Wrote normalized PES values to WAV file

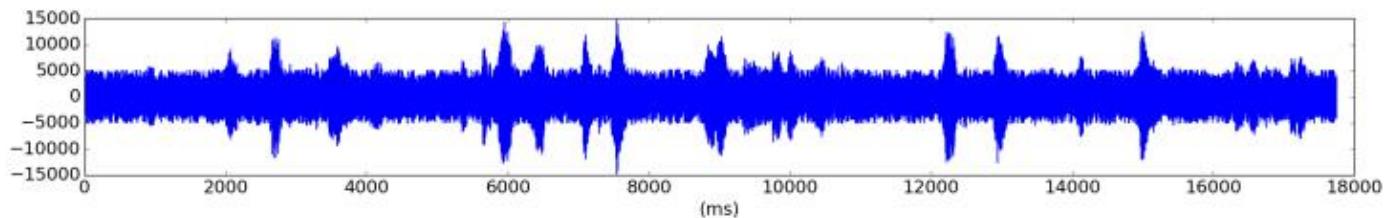
Noise from:

- Platter eccentricity
- Thermal drift
  - Errors 300X width of track
- turbulence

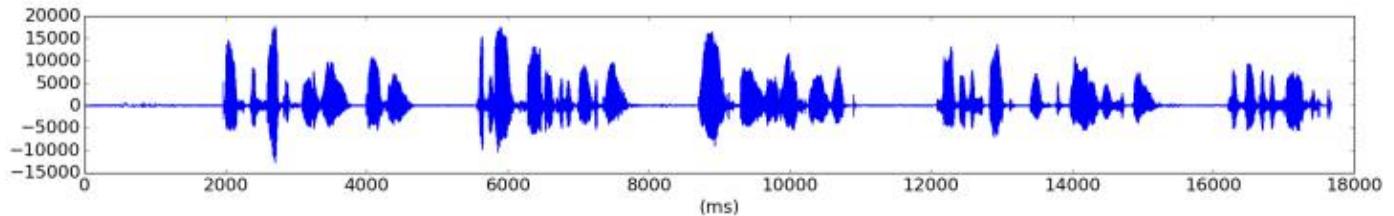


# Signal Analysis

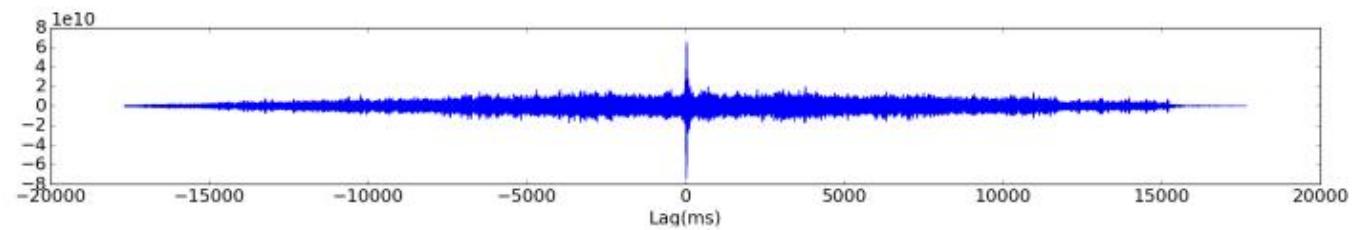
From HDD:



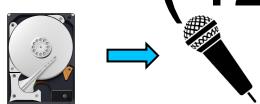
Original:



Cross  
Correlation:



- Harvard Sentence male speaker with drive enclosed in case and fan powered at max (42W)



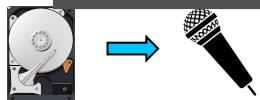
# Quantitative Measures

PESQ MOS: Perceptual Evaluation of Speech Quality.

- Estimates intelligibility of speech
- Baseline: 1.7dB
- From exposed HDD: 1.4 dB
- Inside external hard drive enclosure: 1.6 dB

Enclosure actually improved results!

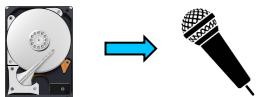
- Container presents a larger surface area to oncoming waves



# Speech Sample

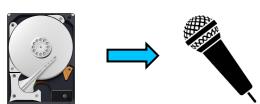
Transcription:

- Paint the sockets in the wall dull green.
- The child crawled into the dense grass.
- Bribes fail where honest men work.
- Trample the spark, else the flames will spread.



# Shazam Recognition

- Played Iron Maiden's "The Trooper" at hard drive



# Success, but ...

---

Required higher volume (90 dBA), filtering didn't work

- Noise-gating discrimination errors ruined spectral fingerprint
- Recovered audio extremely poor
- Still enough information to be recognized



# Potential Improvements

## Multiple Hard drives

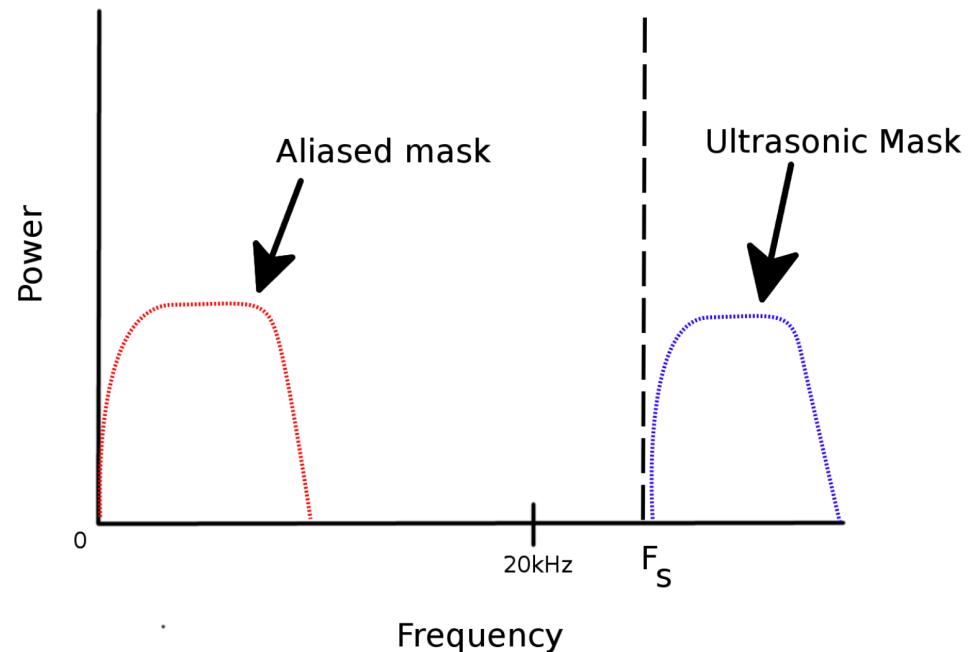
- Make use of signal averaging
- White noise averages to zero, signal averages to itself

Use auto-correlation to find repetitions of same utterance, average them



# Mitigations

- Ultrasonic masking can protect deployed systems
- Sign firmware!
  - Zaddach et al. [3] didn't find signatures in use in any HDDs they examined



[3] [HDD Malware, ACSAC '03]

# Conclusion



Our research sheds light on overlooked threat of devices that weren't designed as sensors



Defenses for already deployed systems are challenging

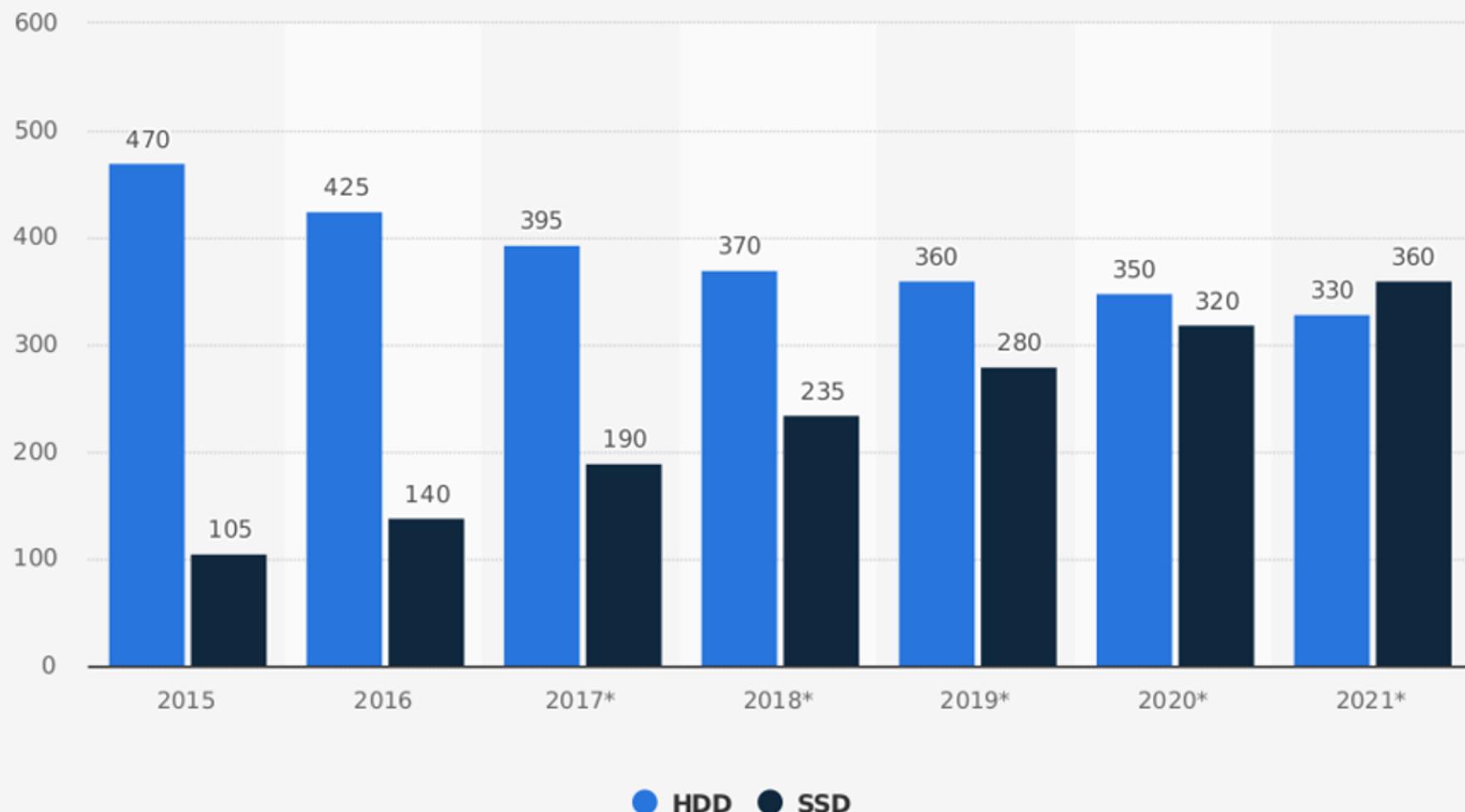


Hard drives can approximate crude microphones



Other Applications: other devices, such as printers; mechanical coupling

## Shipments of hard and solid state disk (HDD/SSD) drives worldwide from 2015 to 2021 (in millions)



### Sources

Statista estimates; IHS (IHS Markit)  
© Statista 2018

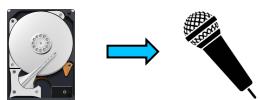
### Additional Information:

Worldwide; 2016



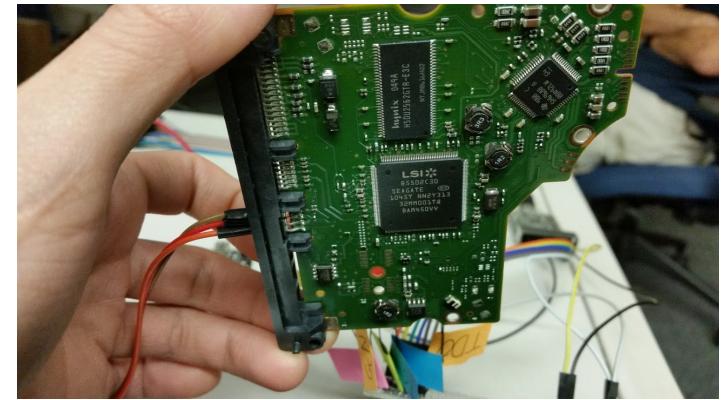
# Granularity

- PES is a 16-bit value
- Granularity:  $1/(2^{12})$  of a track
- Only get 8 bits from AMUX pin
  - Choose bits 3-10



# Accessibility to MCU

- Proof-of-Concept attack demonstrates what an attacker with firmware-resident malware can do
- First confirmed MCU's access to PES

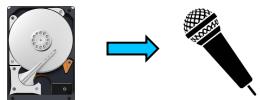


```
File Edit Log Configuration Control signals View Help
3 sigma NRRO = +4.99E-0 % track
**End

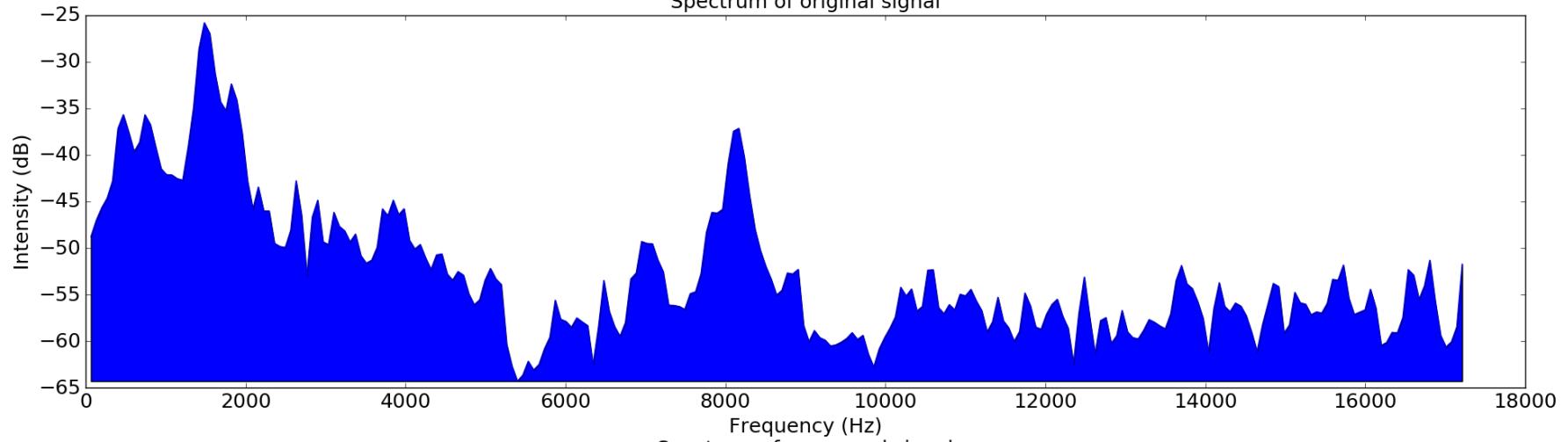
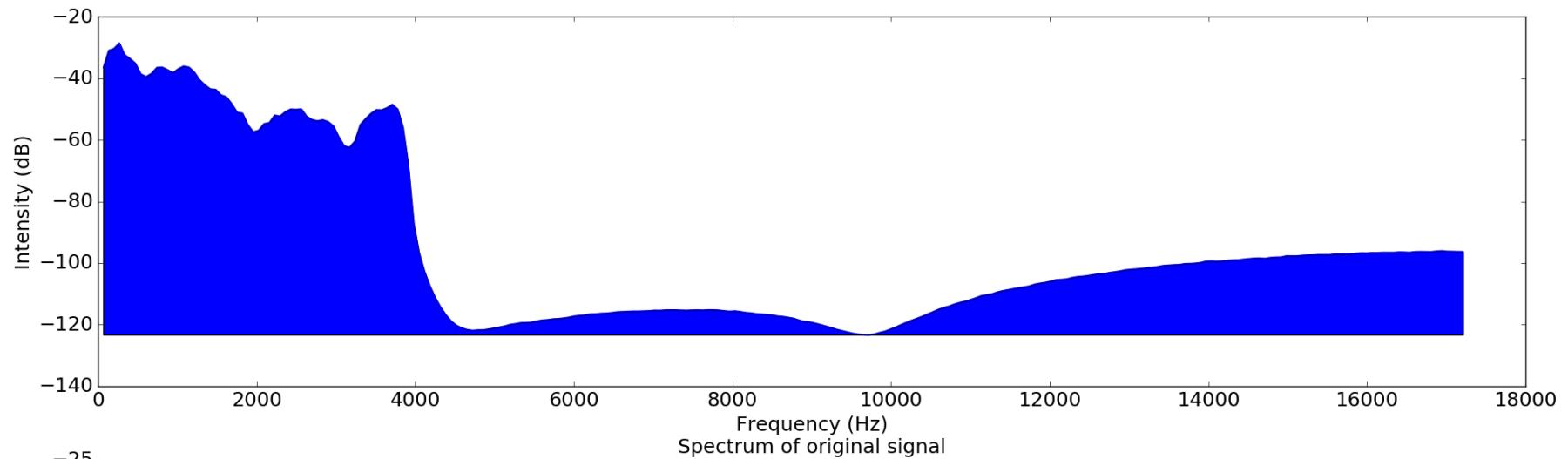
P3 4>U100D
00000.0, WFT 23D (+1.3E+1 %)

00 FF59 0009 008D < - * + >
001 FF1E FFD1 006F < - * | + >
002 FEA0 FF60 0025 < - * | + >
003 FFAD 0046 00F7 < - - | * + >
004 FF73 FFDE 0084 < - - * | + >
005 FF3C 0001 0084 < - - * | + >
006 FF0A FFB1 0029 < - - * | + >
007 FEA8 FF6C 0017 < - - * | + >
008 FF96 002C 00C1 < - - * | + >
009 FF31 FCC6 0057 < - - * | + >
00A FEE0 FF94 0052 < - - * | + >
00B FF03 FCC5 0090 < - - * | + >
00C FF3B FF00 009B < - - * | + >
00D FF69 FFFF 00A3 < - - * | + >
00E FF9D 0037 00E1 < - - * | + >
00F FF75 0021 00BA < - - * | + >
010 FF75 0019 00B1 < - - * | + >
011 FFB0 003E 00C7 < - - * | + >
012 FF38 FFE5 007C < - - * | + >
013 FEE7 FFA0 005C < - - * | + >
014 FF36 FF5F 00B1 < - - * | + >
015 FECF FF87 0047 < - - * | + >
016 FF05 FFB6 0076 < - - * | + >
017 FF60 000C 00B1 < - - * | + >
018 FFDA 006C 0108 < - - * | + >
019 FFD8 0087 0131 < - - * | + >
01A 0005 00A6 0162 < - - * | + >
01B FF9A 0040 00E3 < - - * | + >
01C FF85 001C 00A3 < - - * | + >
01D FF3D FCC1 0056 < - - * | + >
01E FF13 FF97 0027 < - - * | + >
01F FF95 0016 009A < - - * | + >
020 FFBA 004F 0108 < - - * | + >
021 FFEA 009E 0161 < - - * | + >
022 FFFF 0082 011C < - - * | + >
023 0033 00AE 0130 < - - * | + >
024 FF5B FDD0 0065 < - - * | + >
025 FFOF FFBF 0066 < - - * | + >

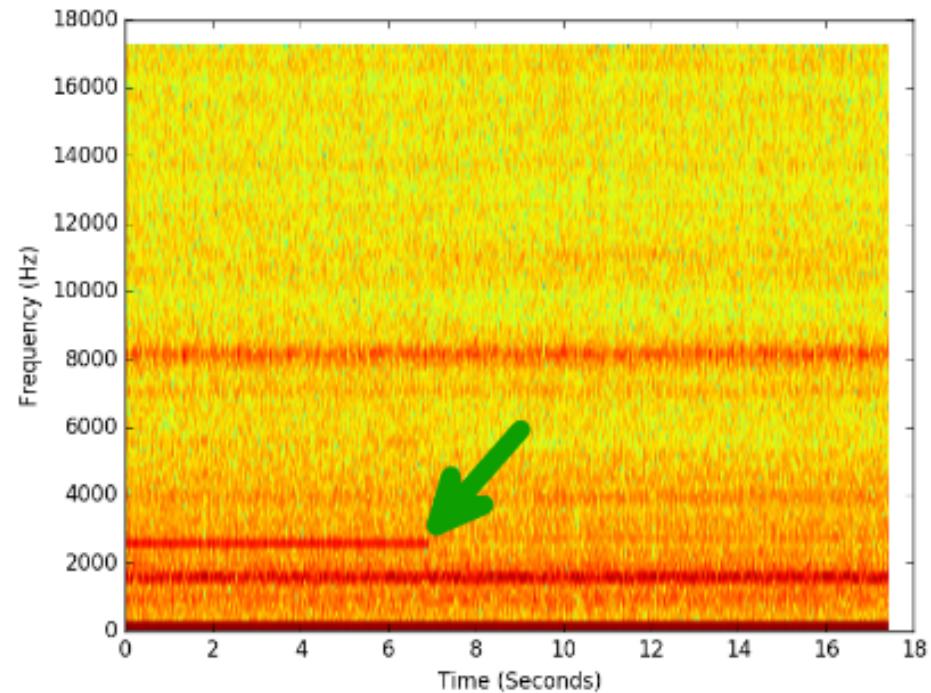
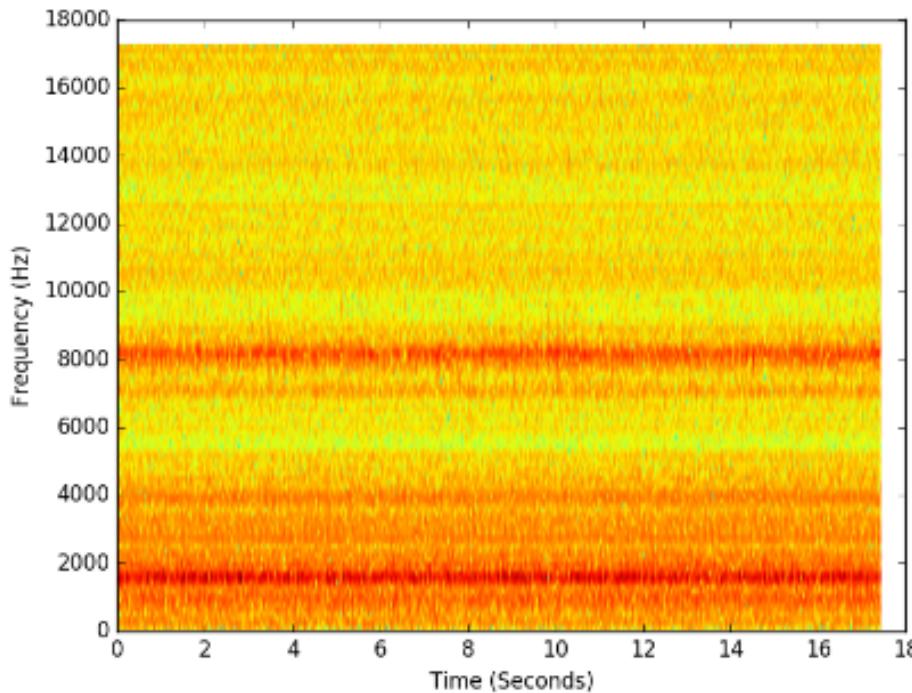
/dev/ttys0 38400-8-N-1
```



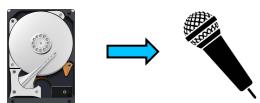
# Frequency Response



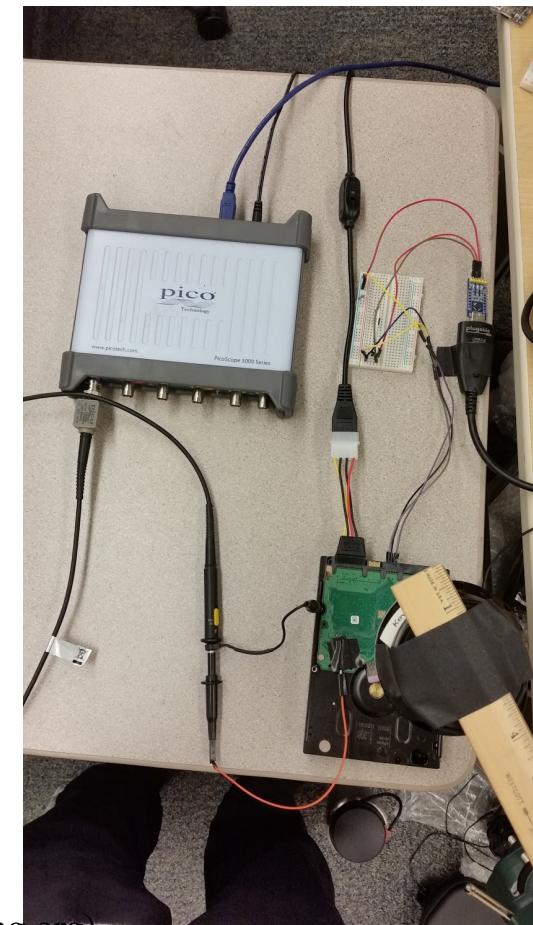
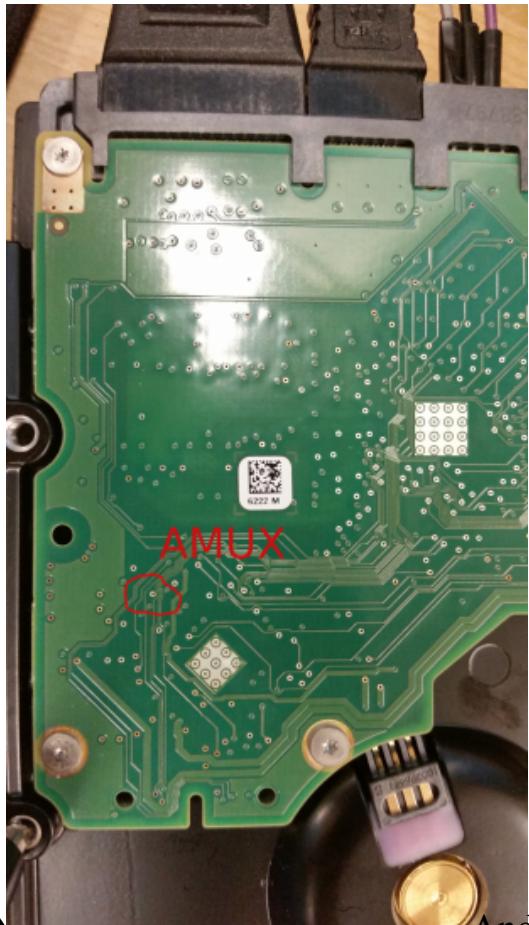
# Spectral Analysis



- Heavy bands of persistent noise around 8 kHz and 1900 kHz
- Responds well to 2.5 kHz tone



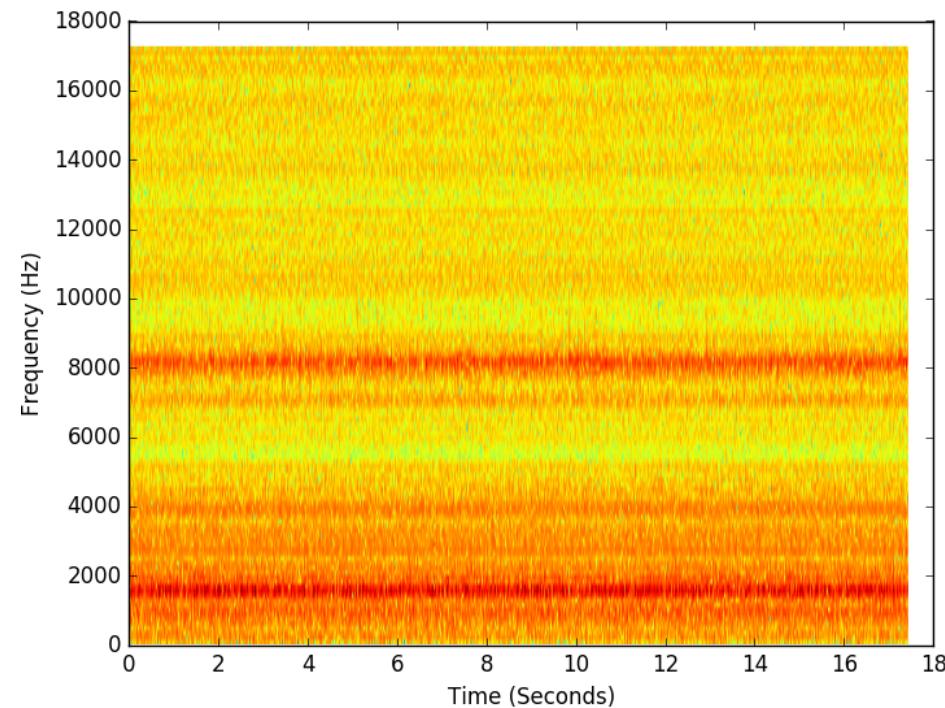
# Reading PES



Andrew Kwong (<https://andrewkwong.org>)

# Digital Signal Processing

---



- Linearly filtering out 8 kHz and 1.9 kHz removes the heaviest bands of noise
- Made use of spectral noise gating for further filtering
  - Find noise thresholds at smaller sub-bands, only pass frequencies above the threshold

